

Order requiring banks and other financial services providers to restrict funding

Q1. What does the order do to restrict the funding?

A: The government declared a public order emergency to take the necessary steps to limit the funding of the activities that led to this current state of emergency.

This order requires all entities such as banks, credit unions, trust and loan companies, cryptocurrency exchanges and anyone providing financial services to take immediate steps to temporarily restrict access to funds to those involved in the blockades.

It requires banks and other financial services providers to cease, suspend or refuse, to provide services to any person or entity involved in the blockades, not to facilitate any transaction relating to funds or virtual currency, and not offer any financial service and providing any funding, including virtual currencies, to anyone involved in the blockades.

Q2. Why is this order necessary?

A: Participants in these activities are receiving funding from various organizations and individuals. The declaration and order aim to put a stop to funding the activities that contribute to the blockades.

Q3. What are banks and other financial services provider required to do under this order?

A: Banks and other financial service providers have to take the following steps:

- Review their records to identify if they have any business with persons involved in the blockades.
- Freeze or suspend business relationships with anyone they identify involved in the blockades. This includes the suspension of access to deposit accounts, cryptocurrency wallets, lending products, and investments.

Q4. Banks have frozen accounts before. What is different?

A: Financial service providers take action on a voluntary basis, which can vary from institution to institution. Currently, they can freeze accounts with a court order and can share information with law enforcement.

The order imposes a set of obligations to review their relationships with anyone involved in the blockades and report to the RCMP or CSIS.

A bank or other financial service provider will now be able to freeze or suspend an account without a court order. In doing so, they will be protected against civil liability.

[APG]

Government of Canada institutions will have a new broad authority to share information with banks and other financial service providers to ensure we all work together to put a stop to the funding of the blockades.

Q5. What safeguards would there be to protect Canadians?

A: These are temporary measures directed at restricting the funding of the blockades and will be in effect for 30 days.

The restriction on funds will cease to apply if affected persons and entities are no longer involved in illegal activities.

Affected individuals will also have access to the courts.

Q6. Will this apply to entities regulated by provinces such as credit unions?

A: Yes, this order applies to all financial services providers, including those regulated under provincial law. This includes provincial credit unions and caisse populaires, provincial companies and securities dealers.

Q7. Does the Order cover cryptocurrencies?

A: The order is broad and covers assets and entities such as digital assets, crypto-currencies, payment processors and funding platforms. This order requires them to take action immediately.

Q8. Is the RCMP be able to share information with banks and other financial entities?

A: The order includes the ability for the RCMP and other provincial (including local police) and territorial law enforcement agencies, together with other institution of the Government of Canada, to share information with banks and other financial services providers if they are satisfied that it will help with implementation of the order.

The information shared could include the names of persons and entities that are involved in the blockades. The RCPM and law enforcement agencies will continue to share information in accordance with their investigation processes.

[APG]

Crowdfunding and payment service provider registration and reporting

Key Messages:

- Under the terms of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), financial institutions and other covered entities are subject to due diligence and disclosure requirements aimed at identifying individuals involved in illicit finance activities.
- Recent activities have highlighted the fact that certain financial service providers, including crowdfunding platforms and the payment service providers they use are not currently subject to the obligations under the PCMLTFA.
- The measures contained in the order extend, for 30 days, the scope of Canada's anti-money laundering and anti-terrorist financing rules to cover crowdfunding platforms and payment processors.
- They require crowdfunding platforms and payment service providers that are in possession or control of any funds that are owned, held or controlled by or on behalf of anyone is engaged, directly or indirectly, in prohibited activities (a designated person) to
 - **Register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC);**
 - **Report suspicious transactions to FINTRAC; and,**
 - **Report large value transactions to FINTRAC.**
- These new requirements will increase the quality/quantity of intelligence received by FINTRAC and the ability of law enforcement agencies to identify and take action against those involved in illicit finance activities.
- Money Services Businesses that are already registered with FINTRAC, and which meet the criteria above, must also update their registration should they operate a crowdfunding platform or perform functions of a payment service provider.
- The government seeks to mitigate anti-money laundering and anti-terrorist financing risks, while minimizing administrative burden, and respecting privacy laws and the Charter of Rights and Freedoms.

Q: What would these changes mean in practice?

A: Extending anti-money laundering and anti-terrorist financing requirements to crowdfunding platforms and the payment service providers they use will not modify the powers of the Minister of Finance or the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). It will ensure that these entities:

- Register with FINTRAC;
- Report any transactions totaling \$10,000 or more;
- Report any suspicious transactions to FINTRAC.

This will help mitigate risks that these platforms receive illicit funds, increase the quality/quantity of intelligence received by FINTRAC, and make more information available to support investigations by law enforcement.

[APG]

Q: What are the limitations of these changes?

A: FINTRAC does not have the authority to track or monitor financial transactions in real time, nor does it freeze assets or investigate potential criminal activities. The RCMP and other policing bodies would remain responsible for investigating crime.

While foreign crowdfunding platforms and the payment service providers they use are captured, enforcement of regulatory requirements could be more limited. For example, there is no ability for FINTRAC to directly examine entities located outside of Canada as the Government of Canada does not have the jurisdiction to do so, and the ability to enforce administrative monetary penalties will be restricted. However, similar to existing requirements for foreign money services businesses, there is a requirement for registration with FINTRAC and to have an officer/office in Canada. This means that FINTRAC will have access to someone located in Canada for the purposes of enforcing regulatory requirements.

The obligations are not being applied retroactively.

Q: How quickly will these new requirements come online?

A: All the authorities in the Order came into force on February 15.

Q: Do these changes cover the use of cryptocurrencies?

A: Yes. Anti-money laundering and anti-terrorist financing requirements under the PMLTFA already apply to virtual (crypto) assets, including customer due diligence, recordkeeping, and reporting large value and suspicious transactions.

Cryptocurrency exchanges and custodial cryptocurrency wallet service providers are subject to the Order. Cryptocurrency exchanges are included under the Order as a money services business dealing in virtual currency. These businesses are required to monitor whether they have control of property that is held on behalf of individuals or entities involved in the illegal blockades and to cease providing exchange and transfer services upon making such a determination. They are also required to register with, and report suspicious and large value transactions, to FINTRAC. The same requirements apply to custodial cryptocurrency wallet service providers.

Q: What is the scope of a “money services business dealing in virtual currency”?

A: It includes persons or entities that are engaged in the business of providing virtual currency exchange services and virtual currency transfer services.

- Virtual currency exchanges services includes exchanging funds for virtual currency, virtual currency for funds or, virtual currency for another virtual currency
- Virtual currency transfer services includes transferring virtual currency at the request of a client and receiving a transfer of virtual currency for remittance to a beneficiary

[APG]

It includes foreign money services businesses that provide virtual currency exchange services and virtual currency transfer services to persons or entities in Canada

It includes custodial virtual currency wallet providers

- Custodial virtual currency wallets are wallets where a private key is held by a third party (e.g., Binance or Coinbase) or where there exists some other measure of control over the virtual currency

Q: What is excluded from the scope of a money services business dealing in virtual currency?

A: Non-custodial virtual currency wallets cannot be subject to the requirements under the Order because they do not have any control or ability to access the virtual currency.

[APG]

Annex – Background Information

CROWDFUNDING

- **Crowdfunding** is the practice of funding a project or venture by raising financial contributions from a number of people, typically through online platforms, in order to carry out a project, investment or other endeavor requiring funds. Crowdfunding campaigns are often completed in conjunction with a dedicated crowdfunding platform or by initiating informal appeals through social media. A crowdfunding platform, also called a funding portal, posts crowdfunding projects on its website. Estimates of the sector vary. Globally, the crowdfunding industry is estimated to be worth US\$10.2 billion in 2018 and is expected to reach US\$28.8 billion by the end of 2025.
- Unlike traditional fundraising methods (e.g. loans from financial institutions), crowdfunding allows individuals or groups to appeal for funds directly from members of the public. Crowdfunding platforms enable those connected online or through social media, who may be geographically dispersed, to pool resources towards common goals and projects that require financing.

PAYMENT SERVICE PROVIDERS

- **Payment service providers (PSPs)** include a variety of entities that perform electronic payment functions, such as payment processors, digital wallets, currency transfer services, and other payment technology companies that offer any of the following services:
 - providing and maintaining a payment account;
 - holding funds until the end user withdraws or transfers them;
 - initiating an electronic funds transfer as requested by an end user;
 - authorizing or transmitting instructions about an electronic funds transfer; and
 - clearing or settling electronic funds transfers
- Many of the crowdfunding platforms that currently exist use third party **PSPs** to enable the completion of payments. This means that the information related to the transaction as well as the movement of money itself, is fragmented along a number of different entities, but would most likely be held with the PSP, rather than the crowdfunding platform lending its services to an individual or entity engaged in fundraising.

CROWDFUNDING AND FINTRAC DATA

- Under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, *FINTRAC does not have the authority to track or monitor financial transactions in real time.*
- *The Centre receives approximately 30 million financial transaction reports a year from businesses subject to the Act, including reports on international electronic funds transfers (EFTs) totaling \$10,000 or more within a 24 hour period; large virtual currency transactions totaling \$10,000 or more within a 24 hour period; and suspicious transactions, which have no monetary threshold for reporting.*

[APG]